IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	Atty. Docket No: 35997-215058
Bruno Couillard	Art Unit: 2137
Application No: 09/919,958	Examiner: M. J. Pyzocha
Confirmation No: 4261	Customer No: **26694** PATENT TRADEMARK OFFICE
Filed: August 2, 2001	

For: **METHOD AND SYSTEM FOR SECURELY TIMESTAMPING DIGITAL DATA**

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

As required under § 41.37(a), this brief is filed more than two months after the Notice of Appeal filed in this case on October 16, 2006, and is in furtherance of said Notice of Appeal.

A one month Extension of Time is hereby petitioned, and is accompanied with the appropriate fee. The fees required under § 41.20(b)(2), and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1206:

01/16/2007 JADD01 00000063 220261 09919958
01 FC:1402 500.00 DA

I.	Real Party In Interest
II	Related Appeals and Interferences
III.	Status of Claims
IV.	Status of Amendments

V. Summary of Claimed Subject Matter
VI. Grounds of Rejection to be Reviewed on Appeal
VII. Argument
VIII. Claims
IX. Evidence
X. Related Proceedings
Appendix A Claims

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is:

Safenet, Inc.

4690 Millennium Drive

Belcamp, Maryland 21017

II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Total Number of Claims in Application

There are 23 claims pending in the application.

B. Current Status of Claims

1. Claims canceled: 7, 19.
2. Claims pending: 1-6, 8-18, 20-25.
3. Claims rejected: 1-6, 8-18, 20-25.

C. Claims On Appeal

The claims on appeal are claims 1-6, 8-18, and 20-25.

IV. STATUS OF AMENDMENTS

Applicant filed a Second Request for Reconsideration on September 15, 2006, and a Notice of Appeal on October 16, 2006. Applicant did not file an Amendment After Final Rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Embodiments of the invention provide a method and system for securing timestamping of digital data. Embodiments of the present invention provide numerous advantages over known methods for time-stamping digital data. Advantages of the invention are described in the specification at page 7, paragraph 27, for example. The advantages include preventing validation of a false time stamp, for example, when a dishonest person provides a document together with false time data for encryption using the encryption key of a timestamping module.

These and other advantages are achievable with embodiments of the present invention as recited, for example, in independent claim 1. As recited in independent claim 1, a method for securing timestamping of digital data is provided. Conventional timestamping systems and methods are based on the steps of providing a document, hashing the document, providing time data and encrypting the hashed document with the time data using an encryption key of a timestamping module. When the encrypted data is decrypted the timestamping module verifies the timestamp as accurate. However, problems arise because conventional techniques are prone to tampering during a test of a timestamp module, or before a key is designated for timestamping purposes only. For example, if there is a secure key for use in encryption stored within a module, false time data could be passed along with a document. The document is hashed and the false time data and the document are encrypted with the secure key. The result looks like a timestamp. If that secure key later becomes a timestamping key or is set to timestamping by a dishonest person tampering with the timestamping module there is no guarantee that a timestamp is authentic.

As recited, for example, in claim 1, a secure encryption key is provided, as well as a processor for performing security functions with the secure encryption key. The processor is operable in a first mode, where the secure encryption key is used for encryption operations and for test operations. The procesor is operable in a second mode in which the secure encryption key is only used for timestamping operations. Once the processor performs a function with the secure encryption key in the second mode, it is precluded from performing further functions in the first mode with the same secure encryption key. Please see page 6, paragraph 26, and Figure 1 of the specification.

Independent claim 11 recites steps similar to claim 1, and further recites when the processor is in the first mode of operation, receiving a first request to perform a timestamping operation on first digital data and then placing the processor in the second mode of operation, and providing a unique code for being embedded within timestamped digital data, the unique code being indeterminable before receipt of the first request. The changing of processor operation mode and the generation of the unique code has the advantage of preventing falsification of time data that is forward in time. Please see, e.g., page 7, paragraphs 28-29.

Accordingly, embodiments of the invention provide a method and system for securing timestamping of digital data.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether the Examiner has established that claims 1-6, 8-18, and 20-25 are obvious over Fischer (U.S. Patent No. 5,001,752), in view of Goodman (U.S. Patent No. 5,001,752), in view of Menezes (Handbook of Applied Cryptography), and in view of Nakamura (U.S. Patent No. 6,457,126).

VII. ARGUMENT

Fischer teaches a public-key date/time notary device for performing secure timestamping of digital messages. See Fischer, Abstract. In FIG. 1, Fischer discloses a processor module 6 coupled to a storage device 8. The storage device stores a secret private key of a public/private key pair. See Fischer, col. 4, lines 35-38. A document presented for notarization receives a timestamp generated by the processor module using the time data output from one or more clocks. See Fischer, col. 5, lines 41-55. The processor uses the secret key S for signing the digital document, including a time stamp value V1. See Fischer, col. 6, lines 14-24. Fischer does not teach or disclose any other modes of operation, other than an initialization mode when the device is initially loaded with key and clock data. See Fischer, col. 7, lines 60-67.

Fischer fails to teach a system having two separate modes (a first mode for encryption operations and for test operations, and a second mode for timestamping operations), and fails to teach using a secure encryption key in the first mode for encryption and test operations and using

the secure encryption key in the second mode for timestamping operations. By extension, Fischer fails to teach that once the processor performs a function with the secure encryption key in the second mode, it is precluded from performing further functions in the first mode with the same secure encryption key.

Goodman is relied upon to teach the two separate modes that Fischer fails to teach. Goodman generally teaches an integrated circuit having an encryption processor 23 in communication with a real time clock 25 for use in time stamping, and with a memory 24 for storing a secure electronic key. See Goodman, col. 4, line 59 to col. 5, line 3. Goodman teaches that the circuit is operable in two modes: a work mode, including both encryption and timestamping, and a test mode. See Goodman, col. 5, lines 12-14. In the two "modes" taught by Goodman, the encryption processor uses a private, not secure, test key in the test mode, and a separate secure electronic key in the work mode (see Goodman, col. 5, lines 14-20; col. 5, lines 62 to col. 6, line 2; col. 6, lines 55-56, also see col. 7, lines 15-28). Thus, Goodman teaches using separate keys in separate respective "modes". Nowhere does Goodman teach using a secure encryption key in a first mode for encryption and test operations and using the same secure encryption key in a second mode for timestamping operations. Goodman, instead, uses a secure key for encryption and timestamping, and a separate, un-secure key for testing. If Goodman is relied upon for teaching two separate modes, then Goodman also teaches using two separate keys, one secure, and one un-secure. Specifically, Goodman does not teach that the encryption processor 23 (or 33, 43, 66) uses a private test key (or a secure electronic key) in a first mode for encryption operations and for test operations and uses the private test key (or the secure electronic key) in a second mode in which the key is only used for timestamping operations.

Further, by extension, Goodman fails to teach that once the processor performs a function with the secure encryption key in the second mode [i.e. timestamping], it is precluded from performing further functions in the first mode [i.e. encryption or testing] with the same secure encryption key. Goodman precludes the processor from performing test mode operations with the same secure encryption key [as used in the timestamping] once the processor has performed encryption or timestamping, because the test mode of Goodman can only be entered from a powered-down state and uses a separate un-secure key. Goodman, col. 5, lines 31-34. Thus,

Goodman teaches away from using the same key in encryption and test operation and in timestamping operations. Embodiments of the invention as claimed specifically prevent the potential abuse that using the same key repeatedly for both encryption and timestamping can allow.

Therefore, Fischer in light of Goodman does not teach all of the claim features. The combination of Fischer and Goodman might teach a device capable of performing encryption, timestamping and test operations. However, such a combination would have two separate keys, one for encryption and timestamping, and another unsecure key for testing. This combination would further not teach that once the processor performs a function with the secure encryption key in the second mode [i.e. timestamping], it is precluded from performing further functions in the first mode [i.e. encryption or testing] with the same secure encryption key, as the Action concedes.

The combination of Fischer and Goodman therefore fails to teach both using a secure encryption key in the first mode for encryption and test operations and using the secure encryption key in the second mode for timestamping operations, and wherein once the processor performs a function with the secure encryption key in the second mode, it is precluded from performing further functions in the first mode with the same secure encryption key. In fact, the combination teaches away from using the same key in encryption and test operation and in timestamping operations.

Menezes is relied upon to teach wherein once the processor performs a function with the secure encryption key in the second mode, it is precluded from performing further functions in the first mode with the same secure encryption key, which Fischer and Goodman fail to teach, alone or in combination. Specifically, Menezes teaches a session key, which is used for a short time period, such as during a single telecommunications connection, after which it is eliminated. Menezes, p. 494, 1st paragraph. Menezes does not specifically teach that a key used in one mode then precludes the key's use in another mode. Menezes also fails to teach or suggest using a secure encryption key in a first mode for encryption and test operations and using the secure encryption key in a second mode for timestamping operations.

The combination of Menezes with Fischer and Goodman might teach a device capable of performing encryption, timestamping and test operations, with a key that might be eliminated

after some time period. However, such a combination would still have two separate keys, one for encryption and timestamping, and another unsecure key for testing. Further, the combination would not cause the key used in timestamping to preclude use of the key in encryption and/or testing. Instead, the result of the combination would have keys that are eliminated after a time period or session.

Therefore, the combination of Menezes with Fischer and Goodman fails to teach or suggest using a secure encryption key in a first mode for encryption and test operations and using the secure encryption key in a second mode for time stamping operations (i.e. using the same key for encryption/test modes and for time stamping), as the Action concedes. The combination also fails to teach wherein once the processor performs a function with the secure encryption key in the second mode, it is precluded from performing further functions in the first mode with the same secure encryption key.

Nakamura is relied upon to teach using a secure encryption key in a first mode for encryption and test operations and using the secure encryption key in a second mode for time stamping operations. Nakamura teaches a storage device including: a flash memory storing a data encrypting key K1; a ROM storing a system key K2; and a processor. Nakamura, col. 7, line 33 to col 8, line 15.

Nakamura describes a test mode. See, e.g. Nakamura col. 11, line 15 to col. 13, line 38. Nakamura discloses ecryption/decryption operations. See, e.g., Nakamura col. 14, lines 23-29. Nakamura does not teach or discuss a timestamping mode. While Nakamura may teach "multiple modes," Nakamura does not teach using a secure encryption key in a first mode for encryption and test operations and using the secure encryption key in a second mode for time stamping operations. Instead, Nakamura teaches using data encrypting key K1 to encrypt data (Nakamura col. 14, lines 23-26), while the testing operation makes no use of a key at all. The testing operation tests the integrity of the storage medium, and is performed in such a way as to prevent the keys from being leaked, but does not itself use the keys. See, e.g., Nakamura col. 17, lines 9-27.

Applicant respectfully submits that this, or any other Nakamura disclosure, fails to teach or reasonably suggest the use of a single key in multiple modes, for example, one mode for test and encryption, and one mode for timestamping, as set forth in claim 1. Nakamura teaches using

a single key in a single mode. There is no teaching or suggestion of using the same key for testing operations, encryption operations and timestamping operations.

The combination of Nakamura with Menezes, Fischer, and Goodman might teach a device capable of performing encryption, timestamping and test operations, with a key that might be eliminated after some time period. However, such a combination would still have two separate keys, one for encryption and timestamping, and another unsecure key (or no key at all) for testing. Further, the combination would not cause the key used in timestamping to preclude use of the key in encryption and/or testing. Therefore, even if combined, the combination of Fischer, Goodman, Menezes and Nakamura fails to teach at least using a secure encryption key in a first mode for encryption and test operations and using the secure encryption key in a second mode for time stamping operations. The Action fails to show how the combination of references teaches or suggests all of the claim limitations of claim 1.

Therefore, the Action does not establish a *prima facie* case of obviousness to reject claim 1 under 35 U.S.C. § 103(a) based on the combined teachings of Goodman, Fischer, Menezes and Nakamura.

Independent claims 11, 15, 20 and 25 each recite similar elements as those discussed above with respect to claim 1, and are allowable for at least the reasons given above for claim 1.

In view of the above discussion, it is clear that the cited references fail to teach or suggest, alone, or in combination, the features recited in the claims. Each of the dependent claims is allowable for at least the reasons as being dependent from an allowable independent claim. For these reasons, the withdrawal of the rejections of claims

Applicant requests reconsideration and withdrawal of the rejection of claims 1-6, 8-18 and 20-25 under 35 U.S.C. § 103(a) as being unpatentable over Goodman, Fischer, Menezes and Nakamura.

VIII. CLAIMS

A copy of the claims involved in the present appeal is attached hereto as Appendix A. As indicated above, the claims in Appendix A do include the amendments filed by Applicant on April 24, 2006.

IX. EVIDENCE

No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the examiner is being submitted.

X. RELATED PROCEEDINGS

No related proceedings are referenced in II above, hence no Appendix is included.

Dated: January 12, 2007

Respectfully submitted,

By: _____

Caroline J. Swindell
Registration No.: 56,784

Jeffri A. **Kaminski**
Registration No.: 42,709

VENABLE LLP
P.O. Box 34385
Washington, DC 20043-9998
(202) 344-4000
(202) 344-8300 (Fax)
Attorney/Agent For Applicant

APPENDIX A

Claims Involved in the Appeal of Application Serial No. 09/919,958

Claim 1. (*Original*) A method for securing timestamping of digital data comprising the steps of:

providing a secure encryption key; and,

providing a processor for performing security functions with the secure encryption key, the processor operable in a first mode wherein the secure encryption key is used for encryption operations and for test operations and in a second mode in which the secure encryption key is only used for timestamping operations,

wherein once the processor performs a function with the secure encryption key in the second mode, it is precluded from performing further functions in the first mode with the same secure encryption key.

Claim 2. (*Original*) A method for securing timestamping of digital data as defined in claim 1, comprising the steps of:

receiving a request to perform a timestamping operation; and,

placing the processor in the second mode of operation once the request is received.

Claim 3. (*Original*) A method for securing timestamping of digital data as defined in claim 2, comprising the step of:

generating a unique code for being embedded within timestamped digital data, wherein the secure encryption key and the processor are within a secure module and wherein the unique code is indeterminable outside the secure module prior to receipt of the request.

Claim 4. (*Original*) A method for securing timestamping of digital data as defined in claim 2, comprising the step of generating a unique code for being embedded within timestamped digital data, the unique code being indeterminable before receipt of the request.

Claim 5. (*Original*) A method for securing timestamping of digital data as defined in claim 4, wherein the unique code is inserted within each timestamped digital data.

Claim 6. (*Original*) A method for securing timestamping of digital data as defined in claim 5, wherein each timestamped digital data comprises a timestamp, and wherein the unique code is encoded within the timestamp.

Claim 7 (*Canceled*)

Claim 8. (*Previously Presented*) A method for securing timestamping of digital data as defined in claim 3, wherein the unique code is generated based on the secure encryption key.

Claim 9. (*Previously Presented*) A method for securing timestamping of digital data as defined in claim 3, wherein the unique code is generated based on a random number.

Claim 10. (*Previously Presented*) A method for securing timestamping of digital data as defined in claim 3, wherein the unique code is generated based on a real time value indicative of a time instance a first request has been received.

Claim 11. (*Original*) A method for securely timestamping digital data comprising the steps of:

providing a secure encryption key;

providing a processor for performing security functions with the secure encryption key, the processor operable in a first mode wherein the secure encryption key is used for encryption operations and for test operations and in a second mode in which the secure encryption key is only used for timestamping operations, wherein once the processor performs a function with the secure encryption key in the second mode, it is precluded from performing further functions in the first mode with the secure encryption key;

when the processor is in the first mode of operation, receiving a first request to perform a timestamping operation on first digital data and then placing the processor in the second mode of operation; and,

providing a unique code for being embedded within timestamped digital data, the unique code being indeterminable before receipt of the first request.

Claim 12. (*Original*) A method for securely timestamping digital data as defined in claim 11, comprising the steps of:

receiving from a real time clock data indicative of a real time the first request for a timestamping operation has been received;

generating a first timestamp based on the data indicative of real time using the secure encryption key;

embedding the first timestamp within the first digital data and inserting the unique code within the first digital data; and,

encoding the first digital data with inserted data therein to form timestamped digital data.

Claim 13. (*Original*) A method for securely timestamping digital data as defined in claim 12 wherein encoding includes the step of encrypting the digital data with the secure key.

Claim 14. (*Original*) A method for securely timestamping digital data as defined in claim 13, comprising the steps of:

receiving a second request to perform a timestamping operation on second digital data;

receiving from the real time clock data indicative of a real time the second request for a timestamping operation has been received;

generating a second timestamp based on the data indicative of a real time using the secure encryption key;

embedding the second timestamp within the second digital data and inserting the unique code within the second digital data; and,

encoding the second digital data with inserted data therein to form timestamped digital data.

Claim 15. (*Original*) A method for securely timestamping digital data comprising the steps of:

providing a secure encryption key;

providing a processor for performing security functions with the secure encryption key, the processor operable in a first mode wherein the secure encryption key is used for encryption operations and for test operations and in a second mode in which the secure encryption key is only used for timestamping operations, wherein once the processor performs a function with the secure encryption key in the second mode, it is precluded from performing further functions with the secure encryption key in the first mode;

placing the processor in the second mode of operation; and,

providing a unique code for being embedded within timestamped digital data, the unique code being indeterminable before the processor is placed in the second mode of operation.

Claim 16. (*Original*) A method for securely timestamping digital data as defined in claim 15, comprising the steps of:

receiving a request to perform a timestamping operation on digital data;

receiving from a real time clock data indicative of a real time value that the request for a timestamping operation has been received;

generating a timestamp based on the data indicative of a real time using the secure encryption key;

embedding the timestamp within the digital data;

inserting the unique code within the timestamped digital data; and,

encoding the digital data with the unique value and the timestamp embedded therein to form timestamped digital data.

Claim 17. (*Original*) A method for securely timestamping digital data as defined in claim 15, comprising the steps of:

receiving a request to perform a timestamping operation on digital data;

receiving from a real time clock data indicative of a real time the request for a timestamping operation has been received;

hashing the digital data; and,

encrypting the hashed digital data with the data indicative of a real time using the secure encryption key.

Claim 18. (*Original*) A method for securely timestamping digital data as defined in claim 17, comprising the step of inserting the unique code within the hashed digital data prior to encryption thereof.

Claim 19. (*Canceled*)

Claim 20. (*Previously Presented*) A secure system for securely timestamping digital data comprising:

at least a first port for receiving the digital data and for providing timestamped digital data; and

a processor for:

performing security functions with a secure encryption key, the processor operable in a first mode wherein the secure encryption key is used for encryption operations and for test operations and in a second mode in which the secure encryption key is only used for timestamping operations, wherein once the processor performs a function with the secure encryption key in the second mode, it is precluded from performing further functions with the secure encryption key in the first mode.

Claim 21. (*Original*) A system for securely timestamping digital data as defined in claim 20, comprising: a real time clock for providing data indicative of a real time.

Claim 22. (*Previously Presented*) A system for securely timestamping digital data as defined in claim 21, wherein the processor comprises circuitry for generating the secure encryption key.

Claim 23. (*Original*) A system for securely timestamping digital data as defined in claim 22, wherein the processor comprises circuitry for generating a pseudo-random number forming a unique value associated with an encryption key, the unique value for being embedded within each timestamp formed with the associated key, the unique value being indeterminable outside the system before the processor is placed in the second mode.

Claim 24. (*Original*) A system for securely timestamping digital data as defined in claim 22, comprising secure memory for storing the secure encryption key inaccessible outside of the secure system but accessible to the processor for performing security functions therewith, wherein within the memory is stored a unique value associated with an encryption key, the unique value for being embedded within each timestamp formed with the associated key, the unique value being indeterminable outside the system before the processor is placed in the second mode.

Claim 25. (*Original*) A system comprising:

a processor that processes a secure encryption key, said processor being operable in a first mode that processes the secure encryption key in encryption operations, and in a second mode that processes the secure encryption key in timestamping operations, wherein once the processor processes the secure encryption key in the second mode, the processor is precluded from processing the secure encryption key in the first mode.